General Services Administration
Information Security Oversight Office
Washington, DC 20405

June 29, 1984

Mr. Harry E. Fitzwater
Deputy Director for Administration
Central Intelligence Agency
Washington, DC 20505

Dear Mr. Fitzwater:

With the fiscal year three-quarters complete, the Information Security Oversight Office (ISOO) is in the thick of its annual inspection schedule. Several matters keep surfacing that require the attention of agency information security management. The enclosed "Notes and Reminders" address these issues. We request that you distribute this information as may be necessary throughout your agency.

One issue predominates. As usual, it is the matter of unnecessary classification, which we usually refer to as overclassification. Notwithstanding the unprecedented decrease in original classification during FY 1983, reported to you earlier in ISOO's FY 1983 Annual Report to the President, the media continue to concentrate their attention on the real or imagined abuses of the system. While ISOO has yet to receive overall statistics for FY 1984, we have noted a disturbing tendency toward questionable classification decisions in our inspections and general oversight. Under these circumstances it is essential that every agency heed the President's instruction "to insure that information is being classified only when this extraordinary protection is necessary . . . ."

Please contact your ISOO liaison if you need greater detail on any of the issues discussed.

Sincerely,

Steven Garfinkel

STEVEN GARFINKEL
Director

Enclosures

Notes and Reminders

1. Overclassification. In the course of ISOO's inspections and general oversight, we seem to be witnessing an increase in the number of questionable classification decisions. As we have noted repeatedly, the issuance of E.O. 12356 was not intended to increase the types or quantity of information that may be classified. Before information may be classified originally, the following tests apply: (a) the person making the classification decision must be an authorized original classifier; (b) the executive branch must own or otherwise control the information to be classified; (c) the information must fall within a classification category listed in Section 1.3(a) of the Order; and (d) the classifier must determine that the unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

   Several of these questionable classifications have involved the application of the so-called "mosaic" principle. The "mosaic" principle occurs when otherwise unclassified pieces of information qualify for classification when combined and examined in their entirety. The use of the "mosaic" to classify information is appropriate only in those unusual circumstances in which the whole is greater than the sum of its parts. This occurs when the cumulative impact of individual pieces of information tends to reveal some additional information which is classifiable, e.g., the identity of an intelligence source. Special attention is required whenever a classification decision is based on the "mosaic" principle. ISOO Directive No. 1 requires classifiers to address in writing the rationale behind each "mosaic" classification.

   Another problem area involves "reasonable doubt" about the need to classify. E.O. 12356 purposely shuns rote determinations in these circumstances; i.e., "When in doubt, don't classify," or "When in doubt, classify." Instead, classifiers should base their determinations strictly through the application of the classification tests listed above. They should not hesitate to consult with other officials who can lend their expertise to the issue of classification.

2. Damage Assessments. Last month ISOO Directive No. 1 was amended to include more detailed instructions on the preparation and requirements of damage assessments following the loss or compromise of national security information. It has come to our attention that many agencies missed the publication of this amendment in the Federal Register. We enclose a copy for your reference. The amendment to the ISOO Directive draws upon the product of the Interagency Group/Countermeasures, chaired by the Deputy Under Secretary

of Defense for Policy, General Richard G. Stilwell. Agencies should revise their internal security regulations as may be necessary to incorporate these requirements.

3. National Security Decision Directive 84 (NSDD-84). Contradictory and confusing media accounts have led some agency officials to conclude wrongly that NSDD-84, "Safeguarding National Security Information," is no longer operative. Only those provisions of NSDD-84 relating to prepublication review and polygraph usage are being held in abeyance by the White House. Agencies should continue implementing the other requirements of NSDD-84, including the execution of the Standard Form 189, "Classified Information Nondisclosure Agreement," by all agency employees and contractor employees cleared for access to national security information. The SF-189 contains no prepublication review requirement. Sufficient copies of the SF-189 should now be available through regular supply channels. ISOO will be monitoring agency compliance as part of its inspections program.

4. Reports of Unauthorized Disclosure. Both E.O. 12356 and NSDD-84 require agencies to notify ISOO of unauthorized disclosures of national security information. ISOO's role is not to investigate "leaks" but rather to determine if a disclosure is the product of a weakness in the information security system. Several agencies have worked out reporting formats with ISOO, and we have noted increased compliance with the reporting requirements. If your agency is not complying with these requirements, we enclose for your information the form that ISOO uses to track reported instances of unauthorized disclosures. This form will give you an idea of the information we need to receive from you. To work out an acceptable format for your submissions, please contact your ISOO liaison.

5. Information Security Program Data. Once again ISOO will be collecting relevant data from all agencies on the Standard Form 311 (rev. 4-83), "Agency Information Security Program Data." These completed forms are due from each agency by October 31, 1984, for the data covering FY 1984. If you require additional copies of the SF-311, please contact your ISOO liaison.

6. Standard Forms. ISOO will very shortly be submitting for your review and comment drafts of several security forms that it is proposing for standardization. Please be prepared to provide us with timely responses.

7. Reclassification. Section 1.6(c) of the Order requires agency heads to notify ISOO whenever they reclassify information that has previously been declassified and disclosed. (This requirement also applies whenever information that has been made available to the public is subsequently classified for the first time.) Because

reclassification actions are inherently controversial, they receive a great deal of outside attention. ISOO has received very few notifications of such reclassifications, and we assume, perhaps optimistically, that minimal reclassification is occurring. Please notify ISOO if you are aware of any reclassification action that has not been reported to us. Our involvement can help prevent a legitimate classification action from becoming an embarrassing front page story.

8. Marking Pamphlet. Because of continued demand, ISOO is reprinting copies of its pamphlet on marking national security information under E.O. 12356. If you are interested in receiving additional copies, please contact your ISOO liaison.

9. ISOO Symposium. Security managers, classifiers, FOIA specialists, public information officers, attorneys, agency historians, and any other persons interested in national security information should hold open **December 5, 1984**. ISOO will be sponsoring a no-cost symposium on that date that will feature prominent speakers and intense debate on the critical issues of information security. Details will follow.